UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

BRANDEN TURNER and BRANDICE TURNER, individually and on behalf of all others similarly situated, Plaintiffs, v. AMERICOLD LOGISTICS LLC, Defendant.	Case No. _____ Judge **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Branden Turner and Brandice Turner ("Plaintiffs"), bring this Class Action Complaint ("Complaint") against Defendant Americold Logistics LLC ("Americold" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Americold's failure to implement reasonable and industry standard data security practices.

2. Defendant is a limited liability company that provides "technology-

based engineered solutions for the temperature-controlled supply chain industry."[1]

3. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices, including, but not limited to names, addresses, driver's license/state ID numbers, passport numbers, financial account information, Social Security numbers ("personally identifying information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

4. Upon information and belief, former and current employees and beneficiaries at Defendant are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, as a condition of becoming employed at Defendant and/or to obtain certain employment benefits. Defendant retains this information for at least many years and even after the relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

[1] https://www.americold.com/

6. According to the Notice of Data Breach letter that Defendant sent to Plaintiffs and other impacted Class Members (the "Notice Letter"), on April 26, 2023, Defendant "became aware of a cybersecurity incident that involved the deployment of malware on certain systems."[2] In response, Defendant "engaged outside counsel, which launched a forensic investigation with the assistance of a leading cybersecurity firm."[3] As a result of the investigation, Defendant concluded—on an undisclosed date—that "on April 26, 2023, an unauthorized party was able to remove some data from the network."[4]

7. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiffs' and approximately 129,000 other individuals' information.[5]

8. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect its employees' and beneficiaries' sensitive data. Hackers targeted and

---

[2] The "Notice Letter". A sample copy is available at https://oag.ca.gov/ecrime/databreach/reports/sb24-577648

[3] *Id.*

[4] *Id.*

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5.shtml

obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. In breaching its duties to properly safeguard its employees' and beneficiaries' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

10. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

11. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an

unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Branden Turner's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and

adequate measures to protect the Private Information.

13. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

14. Plaintiff Branden Turner is and has been, at all relevant times, a resident and citizen of Powder Springs, Georgia. Mr. Turner received the Notice Letter, via U.S. mail, directly from Defendant, dated December 8, 2023. Mr. Turner provided his Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Mr. Turner had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

15. Plaintiff Brandice Turner is and has been, at all relevant times, a resident and citizen of Powder Springs, Georgia. Ms. Turner received the Notice Letter, via U.S. mail, directly from Defendant, dated December 8, 2023. Ms. Turner provided her Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable

safeguards to protect her Private Information. If Ms. Turner had known that Defendant would not adequately protect her Private Information, she would not have entrusted Defendant with her Private Information or allowed Defendant to maintain this sensitive Private Information.

16. Defendant Americold Logistics LLC is a Delaware limited liability company with its principal place of business located in Atlanta, Georgia. Defendant is a resident and citizen of Georgia. Defendant may be served by service of process upon its registered agent for same, CT Corporation System, 289 S Culver St., Lawrenceville, GA 30046-4805.

17. Upon information and belief, Americold Logistics LLC has at least one member, Americold Realty Trust, Inc., that is a resident and citizen of Georgia, with its address at 10 Glenlake Parkway South Tower, Suite 600, Atlanta, Georgia 30328-7250. Americold Logistics LLC is a subsidiary of Americold Realty Trust, Inc.[6]

18. Other members of the Defendant LLC who are only known to Defendant and who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacity of additional members of Defendant LLC if they exist when their identities become known.

[6]https://www.sec.gov/Archives/edgar/data/1455863/000162828020002690/exhibit211q419.htm

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[7]

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant is a limited liability company that provides "technology-based engineered solutions for the temperature-controlled supply chain industry."[8]

[7] According to the breach report submitted to the Office of the Maine Attorney General, 11 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/8a9ff5c2-9ff4-4f8e-bbdf-987d931364c5.shtml

[8] https://www.americold.com/

23. Plaintiffs and Class Members are current and former employees and/or beneficiaries at Defendant.

24. In order to obtain employment and/or certain employee benefits at Defendant, Plaintiffs and Class Members were required to provide sensitive and confidential Private Information, including their names, addresses, Social Security numbers, and other sensitive information.

25. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

26. Upon information and belief, in the course of collecting Private Information from its employees and beneficiaries, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for employee and beneficiary data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

27. Indeed, Defendant's Privacy Notice provides that: "[w]e have implemented appropriate technical and organisational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, and other unlawful or unauthorised forms of Processing, in accordance with applicable law."[9]

[9] https://www.americold.com/wp-content/uploads/sites/2/2021/08/Americold-Privacy-Notice_21-08-05.pdf

28. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

30. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its employees' and beneficiaries' Private Information safe and confidential.

31. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

34. On or about December 8, 2023, Defendant sent Plaintiffs and other victims of the Data Breach a Notice of Data Breach letter (the "Notice Letter"), informing them that:

> **What happened?**
> On April 26, 2023, Americold became aware of a cybersecurity incident that involved the deployment of malware on certain systems. Upon discovery, Americold engaged outside counsel, which launched a forensic investigation with the assistance of a leading cybersecurity firm and reported the matter to law enforcement. Americold subsequently determined that, on April 26, 2023, an unauthorized party was able to remove some data from the network. Based on the comprehensive data analysis that was performed and ultimately completed on November 8, 2023, we were able to determine what information was affected and to whom the information related. As a result of this review, it appears that some of your personal information may have been involved.
>
> **What information may have been involved?**
> The personal information involved may have included name, address, Social Security number, driver's license/state ID number, passport number, financial

> account information (e.g., bank account number, credit card number), and employment-related health insurance and medical information. Please note that not all data elements were involved for all individuals..[10]

35. Omitted from the Notice Letter were any explanation as to why it took Defendant more than *seven months* after detecting the Data Breach occurrence to inform Plaintiffs and Class Members of the cyber attack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

38. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class

[10] Notice Letter.

Members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

39. Plaintiff Branden Turner has been informed by Experian that his Private Information has been disseminated on the dark web, and Plaintiff Brandice Turner further believes that her Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

40. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

41. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like

[11] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

42. To prevent and detect cyber-attacks or ransomware attacks Americold could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities

[12] *Id.* at 3-4.

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[13]

43. Given that Defendant was storing the sensitive Private Information of its current and former employees and beneficiaries, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

44. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of more than one hundred thousand individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, And Stores Plaintiffs' and the Class's Private Information

[13] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

45. As a condition of becoming an employee at Defendant and/or to obtain certain employee benefits at Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information to Defendant.

46. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its business services.

47. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

48. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

50. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

51. Indeed, Defendant's Privacy Notice provides that: "[w]e have implemented appropriate technical and organisational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, and other unlawful or unauthorised forms of Processing, in accordance with applicable law."[14]

Defendant Knew, Or Should Have Known, of the Risk Because Employers In Possession Of Private Information Are Susceptible To Cyber Attacks

52. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting employers that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

[14] https://www.americold.com/wp-content/uploads/sites/2/2021/08/Americold-Privacy-Notice_21-08-05.pdf

54. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[15]

55. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

56. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

[15] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/
[16]https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

57. Additionally, as companies became more dependent on computer systems to run their business,[17] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[18]

58. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

59. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's

[17] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[18] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to more than one hundred thousand individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

63. Defendant's offering of credit and identity monitoring demonstrates that Plaintiffs and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

64. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

65. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

66. As an employer in possession of its current and former employees' and beneficiaries' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to

[19] 17 C.F.R. § 248.201 (2013).

identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

68. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[21] For example, Personal Information can be sold at a price ranging from $40 to $200.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

69. For example, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by

---

[20] *Id.*

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ .

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

70. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number,

[24] Social Security Administration, *Identity Theft and Your Social Security Number, available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

so all of that old bad information is quickly inherited into the new Social Security number."[25]

72. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[26]

73. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[27]

74. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they

[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

[26] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).

[27] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

> want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

75. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[28] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[29]

76. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[30]

77. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed

---

[28] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).

[29] *Id.*

[30] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).

with yours, your treatment, insurance and payment records, and credit report may be affected."[31]

78. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

79. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[32] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[33] In short, these sorts of data breaches are increasingly common, especially among

---

[31] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 6, 2023).

[32] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).

[33] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).

healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[34]

80. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[35]

81. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[36]

82. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[37] Almost half of medical identity theft victims lose their healthcare

---

[34] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed July 24, 2023).

[35] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

[36] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).

[37] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 24, 2023).

coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[38]

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change— *i.e.*, Social Security numbers, PHI, and names. Because the information compromised in the Data Breach is immutable, Plaintiffs and Class Members are at risk of identity theft and fraud for the remainder of their lives.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[39]

---

[38] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

[39] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

85. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

86. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[40]

87. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails To Comply With FTC Guidelines

[40] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

88. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

89. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee and beneficiary information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[41]

90. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[42]

---

[41] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[42] *Id.*

91. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee and beneficiary data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee and beneficiary data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. These FTC enforcement actions include actions against employers, like Defendant.

94. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

95. Defendant failed to properly implement basic data security practices.

96. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its employees' and beneficiaries' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

97. Upon information and belief, Americold was at all times fully aware of its obligation to protect the Private Information of its employees and beneficiaries, Americold was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails To Comply With Industry Standards

98. As noted above, experts studying cyber security routinely identify employers in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

99. Several best practices have been identified that, at a minimum, should be implemented by employers in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer

security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Americold failed to follow these industry best practices, including a failure to implement multi-factor authentication.

100. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Americold failed to follow these cybersecurity best practices, including failure to train staff.

101. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

102. These foregoing frameworks are existing and applicable industry standards for employers' caretaking of employees' and beneficiaries' Private

Information and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

103. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Data Breaches Increase Victims' Risk Of Identity Theft

104. As Plaintiff Branden Turner has already experienced, the unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

105. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

106. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

107. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

108. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[43]

109. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

110. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other

[43] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

111. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

112. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

113. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

114. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and

otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

115. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to take the following measures to protect themselves:

> In addition to activating the complimentary identity monitoring services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and help protect your personal information. We encourage you to remain vigilant over the next twelve to twenty-four months against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid.[44]

116. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the Data Breach upon receiving the Notice Letter, changing passwords and resecuring their own computer networks, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

117. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO

[44] Notice Letter.

Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[45]

118. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[46]

119. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution of Value of Private Information

[45] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[46] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

120. PII and PHI are valuable property rights.[47] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

121. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[48]

122. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[49]

123. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[50,51]

---

[47] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (GAO Report").

[48] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[49] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

[50] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[51] https://datacoup.com/

124. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[52]

125. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[53]

126. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[54]

127. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the

---

[52] https://digi.me/what-is-digime/

[53] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 6, 2023).

[54] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

128. At all relevant times, Americold knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

129. The fraudulent activity resulting from the Data Breach may not come to light for years.

130. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information .

131. Americold was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than one hundred thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

132. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

133. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, and Plaintiff Branden Turner's Private Information already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

134. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

135. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss Of Benefit Of The Bargain

137. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When submitting Private Information to Defendant under certain terms through a job application and/or beneficiary paperwork, Plaintiffs and other reasonable consumers understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received an employment position and/or employee benefits of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Branden Turner

138. Plaintiff Branden Turner is a current employee at Americold.

139. As a condition of obtaining employment at Americold, he was required to supply Defendant with his Private Information, including, but not limited to: his name, address, and Social Security number.

140. At the time of the Data Breach—on or about April 26, 2023—Americold retained Plaintiff's Private Information in its system.

141. Plaintiff Turner is very careful about sharing his sensitive Private Information. Mr. Turner stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

142. Plaintiff Turner received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

143. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff to "remain vigilant over the next twelve to twenty-four months against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid[,]"[55] Plaintiff Turner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon

[55] Notice Letter.

receiving the Notice Letter and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Turner has spent significant time thus far dealing with the Data Breach, including his vacation time for which he was uncompensated for–valuable time Plaintiff Turner otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff Turner suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

145. Plaintiff further suffered actual injury in the form of his Private Information being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

146. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

147. The Data Breach has caused Plaintiff Turner to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed him of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff Turner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Turner is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

149. Plaintiff Turner has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Brandice Turner

150. Plaintiff Brandice Turner receives employee benefits at Americold through her father's (Plaintiff Branden Turner) employment at Americold.

151. As a condition of obtaining employee benefits at Americold, she was required to supply Defendant with her Private Information, including, but not limited to: her name, address, and Social Security number.

152. At the time of the Data Breach—on or about April 26, 2023—Americold retained Plaintiff's Private Information in its system.

153. Plaintiff Turner is very careful about sharing her sensitive Private Information. Ms. Turner stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

154. Plaintiff Turner received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

155. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff to "remain vigilant over the next twelve to twenty-four months against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid[,]"[56] Plaintiff Turner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon

[56] Notice Letter.

receiving the Notice Letter, changing passwords and resecuring her own computer network, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Turner has spent significant time thus far dealing with the Data Breach–valuable time Plaintiff Turner otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

156. Plaintiff Turner suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

157. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

158. The Data Breach has caused Plaintiff Turner to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed her of key details about the Data Breach's occurrence.

159. As a result of the Data Breach, Plaintiff Turner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Turner is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

160. Plaintiff Turner has a continuing interest in ensuring that her Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

161. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

162. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in December 2023 (the "Class").

163. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

164. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

165. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 129,000 persons were impacted in the Data Breach.[57] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

[57] https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5.shtml

166. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

167. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

168. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds

generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

169. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

170. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit

the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

171. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

172. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

173. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

174. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

175. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

176. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard employee Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

177. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 176 above as if fully set forth herein.

178. Defendant requires its employees and beneficiaries, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

179. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its employees, which solicitations and services affect commerce.

180. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

181. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

182. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

183. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

184. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements

discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

185. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment and/or employee benefits at Defendant.

186. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

187. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

188. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' and beneficiaries' Private Information it was no longer required to retain pursuant to regulations.

189. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

190. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession

might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

191. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former employees' and beneficiaries' Private Information it was no longer required to retain pursuant to regulations,

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

192. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

193. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

194. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

195. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

196. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

197. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employers in possession of Private Information.

198. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

199. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

200. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

201. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

202. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

203. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

204. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

205. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

206. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class.

The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

207. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Branden Turner's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

208. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or

harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

209. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

210. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

211. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

212. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

213. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 176 above as if fully set forth herein.

214. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

215. As an employer in possession of the sensitive Private Information of its employees and beneficiaries, Defendant owed a duty of care in protecting Plaintiffs' and Class Members' Private Information, pursuant to Section 5 of the FTC Act, similar state statutes, and an independent duty of care.

216. In its Privacy Notice, Defendant promises employees and beneficiaries that it will not disclose their Private Information, outside of the excepted circumstances set forth therein–-none of which apply here. However, Plaintiffs' and Class Members' Private Information has been disclosed without their written authorization as a result of the Data Breach.

217. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures and Privacy Notice to Plaintiffs and Class Members.

218. Defendant violated Section 5 of the FTC Act and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

219. Defendant violated Section 5 of the FTC Act by negligently misrepresenting its data security practices to Plaintiffs and Class Members.

220. Defendant violated Section 5 of the FTC Act by breaching its duties of care to Plaintiffs and Class Members, as provided in its Privacy Notice.

221. Defendant's violation of Section 5 of the FTC Act and other duties (listed above) constitutes negligence *per se*.

222. Class members are consumers within the class of persons Section 5 of the FTC Act and similar state statutes were intended to protect.

223. Moreover, the harm that has occurred is the type of harm the FTC Act and similar state statutes were intended to guard against.

224. Indeed, the FTC has pursued over fifty enforcement actions against financial institutions which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

225. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

226. There is a close causal connection between Defendant's failure to implement or ensure security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

227. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Branden Turner's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages; (x) nominal damages; and (xi) the continued and

certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

228. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Private Information from a foreseeable and preventable cyber-attack.

229. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

230. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiffs and Class Members damaged other property, including the value of their Private Information.

231. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

232. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

233. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

234. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 176 above as if fully set forth herein.

236. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of their employment at Defendant and/or to obtain certain employee benefits at Defendant.

237. Plaintiffs and Class Members provided their labor to Defendant and/or their Private Information to Defendant in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure.

238. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

239. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

240. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the

Private Information only under conditions that kept such information secure and confidential.

241. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of their employment at Defendant and/or to obtain employee benefits at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

242. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

243. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

244. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

245. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

246. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

247. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

248. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

249. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

250. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

251. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 176 above as if fully set forth herein.

252. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breaches when there is no breach of a contract's actual and/or express terms.

253. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

254. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard employee and benficiary Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

255. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

256. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 176 above as if fully set forth herein.

257. Plaintiffs bring this claim in the alternative to their breach of implied contract claim above.

258. Plaintiffs and Class Members conferred a monetary benefit to Defendant in the form of the providing their Private Information to Defendant, without which Defendant would be unable to conduct its regular course of business.

259. Defendant knew that Plaintiffs and Class Members conferred a monetary benefit to Defendant and they accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Private Information to Defendant from Plaintiffs and Class Members is an integral part of Defendant's business. Without collecting and maintaining Plaintiffs' and Class Members' Private Information, Defendant would be perform its services.

260. Defendant was supposed to use some of the monetary benefit provided to it by Plaintiffs and Class Members to secure the Private Information belonging to Plaintiffs and Class Members by paying for costs of adequate data management and security.

261. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class Members because Defendant failed to implement necessary security measures to protect the Private Information of Plaintiffs and Class Members.

262. Defendant gained access to the Plaintiffs' and Class Members' Private Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

263. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendant had they known of the inadequate security measures.

264. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

265. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Branden Turner's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

266. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

267. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the

interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Americold can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective

responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, pursuant to O.C.G.A. Section 13-6-11, and as otherwise allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: December 19, 2023.

Respectfully Submitted,

/s/MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Phone: (678) 642-2503
Fax: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

John J. Nelson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorneys for Plaintiffs and Proposed Class Counsel

**Pro Hac Vice Forthcoming*

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson